LLNL-JRNL-645372

Meet a Defender

M. M. Myrick

October 28, 2013

Cyber Scoop

Disclaimer

This document was prepared as an account of work sponsored by an agency of the United States government. Neither the United States government nor Lawrence Livermore National Security, LLC, nor any of their employees makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or Lawrence Livermore National Security, LLC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes.

Name: Matthew Myrick
Email: myrick3@llnl.gov
Phone: 925-422-0361

Matthew's journey at Lawrence Livermore National Laboratory began in 1997 when he was selected to participate in the Lab's Engineering Outreach program by his high school accounting teacher. He worked after school and during summer and winter breaks while continuing his education at junior college. As he progressed through school, Matthew took on progressively more difficult tasks, beginning as an administrative assistant's assistant, becoming a summer intern, web developer, system administrator, and software engineer. Then in 2003, it became clear that his passion was in cyber security and he began doing work for the Cyber Security Program (CSP) and hasn't stopped since. In 2004, Matthew graduated from California State University, Chico with an M.S. in Computer Science and, in February 2005, was hired full-time as a member of the Lab's Network Security Team. Currently, Matthew is a Senior Security Engineer and member of the Lab's incident response team. He thrives on the dynamic nature of cyber security and loves the variety of challenges his position offers including incident response, mentoring interns, cyber research, architecting novel defenses, and whatever else comes his way!

Question 1: What tool or system has been most useful for your cyber defense work and why?

The tool that has been most useful for our cyber defenses has been Splunk. I have to admit, I was apprehensive at first because Splunk™ couldn't do anything that I couldn't already do with a few hours of scripting. However, at the insistence of national lab colleagues (thank you guys!), I finally realized the power of Splunk! The Splunk framework levels the playing field for analysts of varied skill levels so they too can assist and respond to cyber incidents. Additionally, Splunk empowers our analysts to unify and refine our cyber approach and our tool chain so that we can focus on what's important...the data.

Question 2: What is the biggest issue you face in cyber defense and how would you fix it?

The biggest issue we face in cyber defense is educating our users. Security isn't a product that can be purchased; security is about the culture of the people. We must teach people to alter their approach and integrate security into their daily routines (not only limited to things that are technology related). To help solve this problem, I believe companies should invest more money and effort into educating their workforce. We can buy every piece of security technology known to man, but until we solve the weakest link (the human) we will always be vulnerable.

Lawrence Livermore National Laboratory is operated by Lawrence Livermore National Security, LLC, for the U.S. Department of Energy, National Nuclear Security Administration under Contract DE-AC52-07NA27344.